- Patch Management -

October 29, 2003

Introduction

High Level Briefing

Third Party Evaluation of Patch Management at FSA

Third Party Evaluation of Products

- No binding ties to vendors

Topics

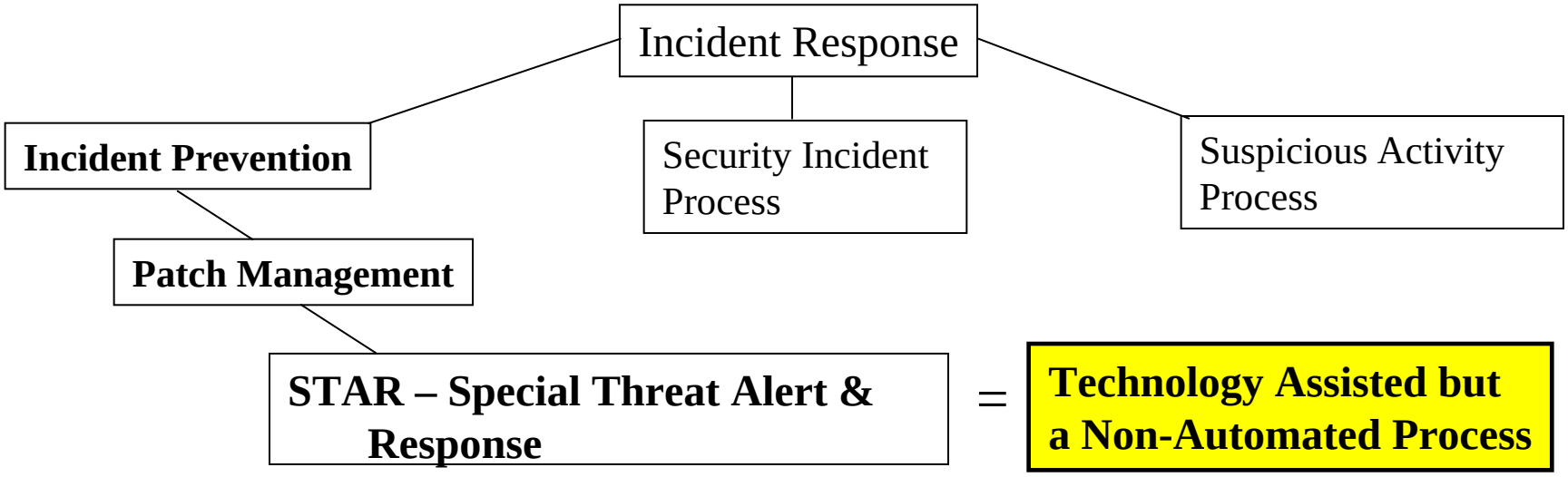
1. What is Patch Management?
2. Current Patch Management at FSA – Non-Automated.
   - *FSA Security Incident Implementation Guide*
3. Configuration Management Program Necessary
4. Automated Patch Management Tools and How They Work
5. Lead Patch Management Products: *PatchLink and BigFix*
   - *Benefits*
   - *Costs*
   - *Implementation Process*

What is Patch Management (PM)?

- Patch Management is the **management** method used to **ensure** that all components of your system have been **updated** to a level that meets your business and security needs.
- To do this effectively a system owner must be able to:
  - Accurately assess inventory and risk
  - Safely test and package solutions (patches)
  - Quickly deploy and verify deployment of the solution
  - Monitor compliance
  - Report on various levels to assess compliance

Patch Management at FSA

From a security perspective Patch Management is included as a part of Incident Response.
The FSA Incident Response Implementation Guide, Section 2 provides the specific procedures FSA system personnel currently need to follow.



"Through 2005, 90 percent of cyber-attacks will exploit known security flaws for which a patch is available or a solution known." **GartnerG2 – May 2002**

Configuration Management (CM)

"You can't…get a patch for stupidity" **Kevin Mitnick (Former Hacker) March 2003**

- Configuration Management
- Change Management
- Release Management

Review Boards need to include an IT security person.

A full scale configuration management program provides a safety feature, a double check, on configuration and security controls.

Automated Patch Management Tools and How They Work

- Inventory all components of your network: Software, Firmware, Hardware.
- Access to current patches either on local server or via remote download.
- Compare your inventory with known fixes – hot fixes, patches, updates
- Show which of your components need to be updated.
- "Package" the fix and send it only to the component(s) that need it.
- Re-inventory components to verify that the fix is applied.
- Continuously monitor the network and system components
- Provide various levels of reporting

Common Areas of Patch Management Comparison

Automated VS. Automatic	Agent based VS. Agent-less	Central (socialized) VS. Distributed

PM Leaders – PatchLink and BigFix

Benefits

PatchLink

Agent based

Consistently ranked as #1 in reviews

- Broadest Support of OS types
- Caches critical patches on server
- Ease of use
- Best price
- Best patch recognition
- Baseline feature
- Can create own patches

BigFix(SecureInfo)

Agent based

Consistently ranked as #2 in reviews

SecureInfo EVM Product is the FEDCIRC PADC program

Unified Products (reporting, patching, C&A)

PatchLink and BigFix – continued 2

Costs

PatchLink
Annual Fees: $12 -$15 per node (everything with agent on it)
One Time Fee: $1,249 per PatchLink server software

BigFix (SecureInfo)
Annual Fees: $25-50 per node

Both solutions may require a full or part-time patch manager. This could result in a net savings as system administrators productivity increases.

PatchLink and BigFix – continued 3

Implementation Process

Assess Scope of Project
Patch Manager and Staff?
Training
Purchase Server/Hardware
Load Software on Servers
Harden the Server (OS and IIS)
Load PM agents
System Now Active
Database builds – reports generated
Work with data to identify Risk Based Decision systems and components

Next Steps?

- **Vendor Demonstrations**
- **Assess what contractors are currently doing for Patch Management.**
- **Decide what Patch Management product and architecture/ implementation will be used.**
- **Modify Contracts if necessary**
- **Integrate into CM**